

Exhibit 3

Declaration of Class Counsel

In re: Equifax Inc. Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Plaintiffs' Motion to Direct Notice of Proposed Settlement

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

In re: Equifax Inc. Customer
Data Security Breach Litigation

MDL Docket No. 2800
No. 1:17-md-2800-TWT

CONSUMER ACTIONS

Chief Judge Thomas W. Thrash, Jr.

**CLASS COUNSEL'S DECLARATION IN SUPPORT
OF PLAINTIFFS' MOTION TO DIRECT NOTICE OF
PROPOSED SETTLEMENT TO THE CLASS**

Kenneth S. Canfield, Amy E. Keller, and Norman E. Siegel declare as follows:

1. We were appointed by this Court to serve as Co-Lead Counsel for the Consumer Plaintiffs and Interim Class Counsel in the above-captioned MDL. Along with Roy E. Barnes, who serves as Co-Liaison Counsel with lead responsibilities, we have led the Plaintiffs' efforts in the consumer track since our appointment on February 9, 2018. We have personal knowledge of all the matters addressed in this Declaration, including the negotiations that culminated with the filing of the proposed settlement now before the Court.

2. Plaintiffs were represented in the negotiations by a Settlement Committee chaired by Mr. Siegel, who in that capacity had overall responsibility for the negotiations and took the lead on our side of the table. Mr. Canfield and Ms. Keller are members of the committee, as are Mr. Barnes and Cam Tribble of the Barnes Law Group. The other members of our negotiating team are Andrew Friedman of Cohen Milstein Sellers & Toll PLLC in Washington, D.C.; Adam Levitt of DiCello Levitt & Gutzler LLC of Chicago, Illinois; James Pizzirusso of Hausfeld, LLP in Washington, D.C.; and John Yanchunis of Morgan & Morgan Complex Litigation Group in Tampa, Florida. The negotiating team was assisted and advised by the Plaintiffs' Steering Committee appointed by the Court, including as needed by other lawyers at their firms. David Berger of the Gibbs Law Group in San Francisco, who has developed a deep expertise in technology matters, provided particular assistance in connection with the business practice changes that are mandated by the settlement.

3. Collectively, the lawyers on our negotiating team have a long history of leading some of the country's most complex civil litigation; have been recognized by courts and national publications for their knowledge and experience in data breach cases; and are responsible for what until this case were the largest data breach settlements in history, including *Home Depot*, *Anthem*, *Yahoo!*, and

Target. Much of this experience was detailed in our leadership application in this case and will not be repeated here. But a brief summary of our experience as it relates to this case may be helpful to the Court.

4. Since the revelation of the Target data breach in late 2013, Mr. Siegel has dedicated much of his practice to representing victims of data breaches. He co-founded the American Association for Justice's Consumer Privacy and Data Breach Litigation Group and previously served as the group's co-chair. He is a nationally published author on emerging issues impacting data breach cases, and he regularly speaks on data breach litigation issues and best practices in settling data breach cases.

5. Mr. Siegel's experience in data breach and consumer privacy cases includes appointment as co-lead counsel for the consumer plaintiffs in *In re: The Home Depot, Inc., Customer Data Security Breach Litigation*, MDL No. 2522, No. 14-md-02583 (N.D. Ga.) (involving a breach affecting more than 60 million customers). In the *Home Depot* litigation, he served as the principal negotiator with Mr. Barnes on behalf of the consumer class that resulted in a settlement that the Court referred to as an "exceptional result" and "the most comprehensive settlement achieved in large-scale data breach litigation." *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, MDL No. 2583, No. 1:14-MD-02583-

TWT, 2016 WL 11299474, at *1 (N.D. Ga. Aug. 23, 2016). He also served as a member of the executive committee and was part of the negotiating team in *In re: Target Corporation Customer Data Security Breach Litigation*, No. 14-md-2522 (D. Minn.) (involving a breach affecting tens of millions of customers), and has worked closely with lead counsel including drafting large portions of the successful standing appeal in *In re U.S. Office of Personnel Management Data Security Breach Litigation*, No. 1:15-mc-01394-ABJ (D.D.C.) (involving a breach of millions of government employee records). He has also served as lead counsel and crafted settlements in smaller data breach cases including *Hutton v. National Board of Examiners in Optometry, Inc.*, No. 16-cv-03025-JKB (D. Md.) (resolving a data breach impacting 60,000 eye doctors across the country; Court finding “multiple beneficial forms of relief . . . reflects an outstanding result for the Class.”).

6. In addition to their extensive experience in many other types of complex litigation and class actions that was described in our leadership application, Mr. Canfield, Mr. Barnes, and Ms. Keller have also litigated and settled major data breach cases. Mr. Canfield served as co-lead counsel in the financial institution track of the *Home Depot* data breach multidistrict litigation before this Court that resulted in what remains the largest data breach settlement

involving banks and credit unions. Mr. Barnes, as noted above, shared responsibility for negotiating the successful settlement of the consumer track in the *Home Depot* breach case. And, both Mr. Canfield and Mr. Barnes serve in leadership positions in *In re: Arby's Rest. Group, Inc. Data Security Litig.*, No. 1:17-cv-1035-AT (N.D. Ga.). Ms. Keller, in addition to her recent appointment as co-lead counsel in the *Marriott* data breach multidistrict litigation, has experience in litigating a number of nationwide consumer class actions. She is a member of the Sedona Conference's Working Group 11, which focuses on litigation issues surrounding technology, privacy, artificial intelligence, and data security, and serves on two drafting teams—one proposing a model data breach notification law, and another opining on statutory damages under U.S. privacy laws, such as the California Consumer Privacy Act.

7. Our colleagues on the Plaintiffs' negotiating team also have extensive backgrounds litigating and resolving data breach cases large and small. Examples of these cases include *In re Anthem, Inc. Data Breach Litig.*, No. 15- MD-02617 (N.D. Cal), which Mr. Friedman led as co-lead counsel and resulted in what until now is by far the largest consumer data breach settlement. Other examples include *In Re: Arby's Rest. Group, Inc. Data Security Litig.*, No. 1:17-cv-1035-AT (N.D. Ga.) (Mr. Pizzirusso); *In re: Yahoo! Inc. Customer Data Security Breach Litig.*,

No. 16-md-02752 (N.D. Cal.) (Mr. Yanchunis); *In re VIZIO Inc. Consumer Privacy Litig.*, No. 8-16-md-02693-JLS (C.D. Cal.) (Mr. Friedman); *In re Sony Gaming Networks and Customer Data Security Breach Litig.*, No. 11-md- 02258 (S.D. Cal.) (Mr. Yanchunis). Including all members of the Plaintiffs Steering Committee, we have collectively handled over 50 data breach cases from coast to coast. [Doc. 187-2] And that record continues—just recently for example, Ms. Keller, Mr. Friedman, and Mr. Pizzirusso were appointed to lead the consumer claim in the *Marriott* data breach multi-district litigation and Mr. Siegel was named to the steering committee.

8. These collective experiences litigating and resolving the largest data breach cases in history were brought to bear on the approach to settling the claims presented in this case, and it is the shared view of the entire Plaintiffs’ Steering Committee that the settlement presented here is historic in several respects. We are confident that this settlement is fair, reasonable, and adequate and in the best interests of the 147 million Americans who were impacted by the 2017 Equifax data breach.

Overview of the Litigation

9. On September 7, 2017, Equifax announced that criminals had stolen from its computer networks confidential personal and financial information

pertaining to about 147 million Americans. Class action lawsuits against Equifax immediately began to be filed by affected consumers and financial institutions. Ultimately, more than 300 such lawsuits were filed around the country. In addition, a few lawsuits were filed by small businesses alleging they had been damaged because their owners' personal information had been stolen in the breach.

10. In December 2017, all of these lawsuits were consolidated by the Judicial Panel on Multidistrict Litigation and transferred to Chief Judge Thomas Thrash, Jr. of the Northern District of Georgia in Atlanta, where Equifax is headquartered. The Court created two separate tracks to manage the litigation — one for the consumer cases (which included claims that had been brought against small businesses) and one for the cases brought by financial institutions. The Court also directed counsel interested in leadership positions in each track to file applications with the Court. There were several dozen applications, some by groups of lawyers and others by individuals. On February 12, 2018, the Court appointed a designated group of 13 lawyers to lead the litigation including Ken Canfield, Amy Keller, and Norman Siegel as Co-Lead Counsel and Roy Barnes as liaison counsel, sharing duties with Co-Lead Counsel. [Doc. 232] This group was also appointed Interim Consumer Class Counsel pursuant to Fed. R. Civ. P. 23(g),

and referred to as “Class Counsel” in the Settlement Agreement and this Declaration.

11. As Class Counsel, our first major task was to file a consolidated amended complaint, which the Court had announced would serve as the vehicle for litigating the consumer claims. Our group had a substantial head start on this task because prior to our appointment we had already filed a case that named class representatives from every state. Nonetheless, the consolidated complaint was a massive undertaking, involving investigating the underlying facts, vetting several thousand potential class representatives, and thoroughly researching many legal theories under federal law and the laws of all 50 states.

12. On May 14, 2018, Plaintiffs filed a 559-page consolidated amended consumer complaint, which named 96 class representatives and asserted numerous common law and statutory claims under both state and federal law. [Doc. 374] Due to the Court’s inclusion of the small business cases in the consumer track, we also filed a separate complaint on behalf of the small businesses. [Doc. 375]

13. In June and July 2018, Equifax moved to dismiss both the consumer and small business complaints in their entirety. [Docs. 428 and 441] Equifax’s primary focus in these motions was attacking Plaintiffs’ negligence and negligence per se claims, arguing that Georgia law does not recognize a legal duty to

safeguard personal information, none of the class representatives (or any class members) suffered a legally-cognizable injury, and Plaintiffs could not plausibly prove any alleged injury was caused by the Data Breach. Both motions to dismiss were exhaustively briefed during the summer and early fall of 2018. [Docs. 452, 471]

14. On December 14, 2018, the Court heard more than three hours of oral argument on Equifax's motions to dismiss. [Doc. 534] On January 28, 2019, the Court issued its rulings granting the motion to dismiss the small business complaint and largely denying the motion directed at the consumer complaint. Equifax answered the consumer complaint on February 25, 2019. [Docs. 540, 541]

15. While the consolidated amended complaints were being prepared and Equifax's motions to dismiss were pending, Class Counsel and the members of Plaintiffs' Steering Committee undertook a substantial amount of other work to move the case forward. That work included the organizational activity that is part of leading any case of this magnitude (establishing committees, assigning areas of responsibility, hiring vendors for e-discovery, etc.), as well as tasks such as locating and consulting with experts; working with the class representatives to assemble their documents and compile their damages; investigating the facts relating to the breach, including the mechanism for how the breach occurred and

the data exfiltrated; communicating with public interest groups active in the cybersecurity, consumer protection, and financial fraud fields; coordinating with the leadership of the financial institution track and the related securities litigation; developing our strategy for prosecuting the case; meeting with state and federal lawmakers regarding the breach; issuing document retention subpoenas to scores of third parties; and attending monthly status conferences in court.

16. Under the local rules of the Northern District of Georgia, discovery does not begin until 30 days after an answer is filed. Nevertheless, we were able to secure case management orders that front-loaded much of the preparatory work needed before formal discovery could as a practical matter proceed, setting the groundwork for discovery once the motions were decided. In accordance with these orders, the parties negotiated a series of protocols to govern discovery, exchanged requests for production of documents, and attempted to negotiate the search terms and list of custodians that would be used in electronic searches. [Doc. 258] (Protective Order); [Doc. 449] (Production and ESI Protocol) Several parts of this pre-discovery process proved to be challenging, forcing Class Counsel to spend substantial time on these matters. On some issues, the parties reached impasse compelling Class Counsel to file a motion seeking limited relief from the

discovery stay and an order facilitating our interviews of former Equifax employees who had signed non-disclosure agreements. [Doc. 488]

17. Once the Court ruled on Equifax's motions to dismiss, Plaintiffs' discovery efforts intensified. Among other things, Class Counsel and Plaintiffs' Steering Committee reviewed approximately 500,000 pages of documents produced by Equifax (along with many thousands of native files including presentations and databases), began producing named plaintiffs' documents to Equifax, and scheduled depositions of several former Equifax employees. Our document review was complicated by Equifax's decision to segregate highly-confidential documents in a "reading room" controlled by Equifax, which involved beginning to negotiate revised orders concerning discovery and creating new review protocols, along with meeting and conferring about Equifax's ongoing productions. Those efforts continued up to the moment the case settled.

Overview of Settlement Discussions

18. In September 2017, Equifax's counsel contacted Mr. Siegel, Mr. Levitt, and others and told us that Equifax was interested in exploring early resolution of the litigation. This led to the formation of a group of Plaintiffs' counsel that decided to work together in an effort to litigate and resolve the case.

This group, with a few additions selected by the Court, was later appointed to lead the consumer track.

19. After initial telephone and in-person discussions regarding a potential settlement process, the parties retained Layn R. Phillips, a former federal judge and principal of Phillips ADR, to serve as mediator. Judge Phillips is perhaps the country's preeminent mediator in major civil litigation and has successfully mediated several other data breach cases, including *In re Anthem Customer Data Breach Security Litig.*, which until now is the most successful consumer data breach settlement. Our first negotiating session took place in Newport Beach, California on November 27-28, 2017. The parties engaged in extensive preparation for the mediation and exchanged comprehensive mediation statements.

20. Based on the collective experiences described above, Plaintiffs presented a paradigm for settlement that would serve as the groundwork for further negotiations: First, Equifax would create a common fund for the benefit of the class that would reimburse class members for out-of-pocket expenses and lost time associated with the breach. Second, class members would be entitled to high quality, three-bureau credit monitoring and identity restoration services. And, third, Equifax would be subject to specific contractual obligations and a related consent order requiring that it substantially reform its data security practices.

21. Although little progress was made at the first mediation, it did serve to initiate what became a lengthy back-and-forth process with Equifax that lasted over the next 16 months. Throughout the process, the three core elements of resolution discussed at the first mediation served as the guideposts that led the parties through various iterations of proposed term sheets, and ultimately the settlement presented by this motion. During the course of 2018, Class Counsel collectively spent more than a thousand hours preparing for and participating in settlement talks, struggling to reach agreement with Equifax on a comprehensive term sheet.

22. The parties negotiated over this period with the oversight of Judge Phillips — work that involved exchanging additional mediation statements, numerous and regular telephone conferences, and additional all-day mediation sessions with Judge Phillips on May 25, 2018, August 9, 2018, November 16, 2018, and March 30, 2019. During this period, Class Counsel and Plaintiffs' settlement committee also spent significant time with vendors so that we could develop and deliver state-of-the-art monitoring and restoration services to the entire class. We also retained several leading cybersecurity experts to assist us and consulted with knowledgeable consumer groups.

23. On a separate track, the parties worked on detailed and comprehensive business practice changes involving Equifax's cybersecurity measures. In connection with the negotiations, we retained Mary Frantz, one of the nation's leading cybersecurity experts. Working continuously with Ms. Frantz, we examined Equifax's existing data security systems, attended multiple meetings at Equifax's headquarters in Atlanta with Equifax's counsel and security experts, and exchanged numerous proposals and counter-proposals regarding improvements to Equifax's data security.

24. Although the negotiations were productive and moved the parties closer to settlement, the process slowed substantially following the November 16, 2018 mediation session, and eventually came to a stop in December. At that point, the parties turned their attention to continuing the briefing and then arguing the motions to dismiss, resulting in a relative standstill on the negotiations pending the Court's ruling on those motions.

25. Following the Court's decision largely denying Equifax's motion to dismiss the consumer claims, the parties renewed negotiations. The meaning and impact of the Court's orders on the prospects of the litigation was hotly debated and prompted the parties to continue their settlement efforts through Judge Phillips. In March 2019, the parties agreed to another mediation session. After

meeting with Equifax's counsel and in-house representatives in California for several hours on the evening of March 29, 2019, and following an all-day mediation session on March 30, 2019, the parties executed a binding Term Sheet that serves as the basis of this Settlement.

26. In between the formal mediation sessions, the parties met several times, engaged in scores of telephone conferences, and exchanged constant emails (Mr. Siegel has over a thousand emails to and from Equifax's lawyers) – all in an effort to move the negotiations forward. At all times the negotiations were at arm's length, sometimes contentious, but always professional.

The Mediated Settlement Terms

27. As discussed above, from the outset of the negotiations, Class Counsel focused on three major components of the settlement. First, the establishment of a cash settlement fund to compensate those class members that had suffered out-of-pocket losses and lost time as a result of the breach. Second, the provision of high quality credit monitoring and identity restoration services. And third, modifications to Equifax's data security practices that would be subject to Court enforcement. The March 30, 2019 Term Sheet achieved all of these goals.

28. The Term Sheet achieved the first litigation goal of securing significant monetary relief through the establishment of a non-reversionary \$310

million settlement fund. The deal was structured so that class members could receive up to \$20,000 with documented losses fairly traceable to the breach, including, but not limited to money spent on placing or removing a security freeze on a credit report with any credit reporting agency; credit monitoring or identity theft protection costs purchased on or after September 7, 2017; unreimbursed costs, expenses, losses, or charges paid on or after May 13, 2017, because of identity theft or identity fraud, falsified tax returns, or other misuse of personal information; other miscellaneous expenses related to any out-of-pocket loss such as notary, fax, postage, copying, mileage, and long-distance telephone charges; professional fees incurred in connection with addressing identity theft, fraud, or falsified tax returns; and up to 25% reimbursement of the money paid for Equifax credit monitoring or identity theft protection subscription products in the year before the breach. The parties also agreed the fund would provide for reimbursement to class members who spent time taking preventative measures or dealing with fraud, identity theft, or other misuse of their personal information for up to 20 hours of time at \$25 per hour. Up to 10 hours of time could be self-certified and not require documentation.

29. The Term Sheet achieved the second key litigation goal in that all class members would be entitled to enroll in three years of three-bureau credit

monitoring services provided by Experian. Comparable products, like Experian's CreditWorks Premium service, retail for \$25 a month (\$300 per year). And, if a class member already had some other kind of monitoring services in place, the Term Sheet provided that class members may file a claim for alternative cash compensation of \$100. In addition, the Term Sheet provided all class members with access to "assisted identity restoration services" if they experience an identity theft event. These services include access to a U.S.-based call center providing services relating to identity theft and fraud restoration. Importantly, class members do not need to file a claim to access these services. Under the Term Sheet, the settlement fund would pay for monitoring for up to seven million enrollees, but Equifax was required to separately pay for all class members who registered in excess of seven million.

30. The Term Sheet achieved the third key litigation goal of requiring Equifax to adopt, pay for, implement, and maintain extensive business practices commitments related to information security to safeguard consumer information for a period of five years, including spending a minimum of \$1 billion on data security and related technology. Over a lengthy period that began in 2017, the information security program was developed by Class Counsel in consultation with Ms. Frantz, and negotiated with Equifax to provide security improvements relating

to data classification, logging and monitoring, vulnerability scanning, penetration testing, patch management, access control and account management, file integrity monitoring, encryption, data retention requirements, and required third party assessments, among many others. Moreover, the Term Sheet provided that an independent third party would assess these commitments and be enforceable in court.

31. The Term Sheet provided for two claims periods – an initial claims period of six months, followed by an extended claims period (if money remained in the fund) for up to three years. At the conclusion of the extended claims period the parties agreed that excess funds would be used for the benefit of the class and could not revert to Equifax. The Term Sheet also delivered another important non-monetary benefit – it provided that Equifax could not seek to enforce any arbitration provision in any Equifax product that has been offered in response to the Data Breach as of the date of the settlement agreement or that is provided under the settlement.

Input from Federal and State Regulators

32. The March 30, 2019, Term Sheet provided for a period of 60 days following the execution of the Term Sheet to allow Class Counsel to consider any comments from the Federal Trade Commission, the Consumer Financial Protection

Bureau, and state Attorneys General (“Regulators”) regarding the relief afforded to the class under the Term Sheet. This provision is consistent with guidance provided by the Federal Judicial Center regarding solicitation of the views of federal and state regulators regarding class action settlements. *See generally*, Federal Judicial Center, Managing Class Action Litigation: A Pocket Guide for Judges at 26-27. Because the Regulators were not involved in negotiating the Term Sheet, the parties agreed that, “to the extent that the Regulators propose changes to the class benefits or the Term Sheet, Plaintiffs will discuss and consider in good faith such changes, and if the parties agree, the Term Sheet and settlement agreement will be amended accordingly.”

33. In the weeks that followed, the Regulators proposed several changes to the substantive terms of the Term Sheet. Some were relatively minor (making clear that consumers could recover for time in 15 minute intervals and increasing the dollar amount for alternative monitoring compensation from \$100 to \$125) while others provided significant additional relief (\$70.5 million for the fund that included money to pay for another year of 3-bureau monitoring and, if needed, \$125 million more to pay excess out-of-pocket claims; 6 years of 1-bureau monitoring through Equifax; and expansion of the Extended Claims Period from 3 to 4 years). Plaintiffs accepted all those proposals. However, Plaintiffs opposed

other proposed changes Class Counsel believed would be the subject of criticism and, in certain instances, might lessen the class benefits in the Term Sheet they had negotiated.

34. These discussions triggered a new round of difficult negotiations that lasted over two months and delayed submitting an agreement to the Court. Through intensive good faith discussions, the remaining issues were resolved, and Class Counsel turned to working with Equifax and the Regulators to refine the notice and claims programs. After numerous conferences with Equifax and the Regulators, and an “all hands” meeting in Washington, D.C. on July 16, the parties were finally able to execute the Settlement Agreement. Like the negotiations with Equifax, all negotiations with the Regulators were arm’s length.

35. Both the Federal Trade Commission and Consumer Financial Protection Bureau also offered helpful suggestions to the notice program and claims administration process. The proposed changes were intended to maximize the efficacy of the notice program, improve accessibility of the notice and claims process, and ultimately increase claims rates. Class Counsel adopted nearly all of these proposed changes, and believe the Regulators’ input improved the final notice program and claims process.

Confirmatory Discovery

36. Following execution of the Term Sheet, Class Counsel engaged in confirmatory discovery related to both the identification of the class and other issues bearing on the settlement. Specifically, Class Counsel sought and received information regarding the specifics of how Equifax determined those individuals impacted by the breach, confirming the mechanism of the breach, and confirming the steps Equifax has taken to improve its data security since the breach was discovered. Specifically, on June 26, 2019, Ms. Keller deposed an employee of Mandiant (the firm that conducted the post-breach investigation) and Equifax's Chief Information Security Officer concerning the breach, Equifax's systems and business practices, and Equifax's post-breach response. The deposition assisted Class Counsel in ensuring that the negotiated settlement relief addresses Plaintiffs' allegations and benefits Settlement Class Members by improving Equifax's security and business practices.

The Settlement Benefits Conferred on the Class

37. Under the proposed settlement, Equifax will pay \$380.5 million into a non-reversionary fund for class benefits, fees, expenses, service awards, and notice and administration costs; and up to an additional \$125 million if needed to satisfy claims for Out-of-Pocket losses if the \$380.5 million fund is exhausted, bringing

the cash fund up to \$505.5 million. Settlement Agreement ¶¶ 3.1 and 3.2. The settlement is structured so that Equifax also may pay into the fund the added costs of credit monitoring if more than seven million class members claim that benefit. These payments could exceed \$2 billion if all class members enroll for this benefit, and accrues at a rate of \$16.4 million for every 1 million enrollees above 7 million. *Id.* at ¶¶ 7.8 and 7.9.

38. The Settlement provides that the fund will provide specific benefits to class members, including:

- Compensation of up to 20 hours at \$25 per hour for time spent taking preventative measures or dealing with identity theft. Ten hours can be self-certified, requiring no documentation. This provision is subject to a \$38 million cap.
- Reimbursement of up to \$20,000 for documented losses fairly traceable to the breach, such as the cost of freezing or unfreezing a credit file; buying credit monitoring services; out of pocket losses from identity theft or fraud, including professional fees and other remedial expenses; and 25 percent of any money paid to Equifax for credit monitoring or identity theft protection subscription products in the year before the breach.
- Four years of specially-negotiated, three-bureau credit monitoring and identity protection services through Experian (a retail value of \$1,200) and an additional six years of one-bureau credit monitoring through Equifax (a retail value of \$720).
- Alternative compensation of \$125 for class members who already have credit monitoring or protection services in place. This provision is subject to a \$31 million cap.

- Identity restoration services through Experian to help class members victimized by identity theft for seven years, including access to a U.S. based call center, assignment of a certified identity theft restoration specialist, and step by step assistance in dealing with credit bureaus, companies and government agencies.

Id. at ¶ 6.2.

39. The documentation necessary to establish Out-of-Pocket Losses may consist of documents such as receipts from third parties, highlighted account statements, phone bills, gas receipts, and postage receipts, among other relevant documentation. Similarly, to obtain Reimbursement for Attested Time of up to 10 hours, class members need only attest to the time spent and briefly describe the actions taken. Claims for Reimbursement for Attested Time of more than 10 hours require documentation, which can be the same documents submitted for Out-of-Pocket losses. If it is not readily apparent how the document establishes a loss, the claimant can provide a brief description of the documentation describing the nature of the loss. *Id.* at ¶ 8.3.

40. If a claim is rejected for any reason, there is also a consumer-friendly appeals process whereby claimants will have the opportunity to cure any deficiencies in their submission or request an automatic appeal if the Settlement Administrator determines a claim for Out-of-Pocket Losses or time is deficient in whole or part. *Id.* at ¶ 8.5.

41. Class members will have six months to file a claim for benefits, but are not required to file a claim to access identity restoration services. *Id.* at ¶¶ 7.2 and 8.1. If money remains in the fund, there will be up to a four-year extended claims period during which class members may recover for Out-of-Pocket losses and time spent rectifying identity theft after the end of the initial claims period. *Id.* at ¶ 8.1.2. Any money remaining after the extended claims period will first be used to pay any claims for time or alternative compensation that were not paid in full because of the caps; purchase up to three years of additional identity restoration services and then to extend the length of credit monitoring for those who claimed that benefit. *Id.* at ¶ 5.4.

42. The credit monitoring product offers class members expansive coverage in monitoring for and protecting against identity theft and fraud. *Id.* at 7.1. Credit monitoring is a service that monitors an individual's credit reports and alerts the individual when any change is made that could signal fraudulent activity. Credit changes can include new credit card or loan applications, new credit inquiries, existing account changes, and new public records or address changes, among others. Credit monitoring gives the individual the opportunity to confirm the accuracy of a credit change in real time and, if necessary, address the issue before fraud occurs or expands.

43. As a separate class benefit, all Settlement Class Members, even those who do not enroll in Credit Monitoring Services or do not submit a claim, will be entitled to utilize identity restoration services offered through Experian. This coverage is a separate benefit and permits all class members to have access to fraud resolution specialists who can assist with important tasks such as placing fraud alerts with the credit bureaus, disputing inaccurate information on credit reports, scheduling calls with creditors and other service providers, and working with law enforcement and government agencies to dispute fraudulent information. Identity restoration services will be available for a period of seven years from the Effective Date of the Settlement Agreement. *Id.* at ¶ 7.2.

44. Equifax has also agreed to entry of a consent order in this action requiring the company to spend a minimum of \$1 billion for cybersecurity over five years and to comply with comprehensive data security requirements as originally provided in the Term Sheet. *Id.* at ¶ 4.1.1. Equifax's compliance will be audited by independent experts and subject to this Court's enforcement powers. *Id.* at ¶ 4.1.2. The components of the business practice changes include:

- **Information Security Program:** Within 90 days of final approval, Equifax shall implement, and thereafter regularly maintain, review, and revise a comprehensive Information Security Program that is reasonably designed to protect the confidentiality, integrity, and availability of the Personal

Information that Equifax collects, processes, or stores on the Equifax Network.

- **Managing Critical Assets:** Equifax shall identify and document a comprehensive IT asset inventory, using an automated tool(s) where practicable, that, consistent with NIST or another comparable standard, will inventory and classify, and issue reports on, all assets that comprise the Equifax Network, including but not limited to software, applications, network components, databases, data stores, tools, technology, and systems. The asset inventory required under this paragraph shall be regularly updated and, at a minimum, identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the Equifax Network; and (e) the asset's criticality rating. Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing that hardware and software within the Equifax Network be rated based on criticality, factoring in whether such assets are used to collect, process, or store Personal Information. Equifax shall comply with this provision by June 30, 2020.
- **Data Classification:** Equifax shall maintain and regularly review and revise as necessary a data classification and handling standard.
- **Security Information and Event Management:** Consistent with NIST or another comparable standard, Equifax shall implement a comprehensive, continuous, risk-based SIEM solution (or equivalent). Equifax shall continuously monitor, and shall test on at least a monthly basis, any tool used pursuant to this paragraph, to properly configure, regularly update, and maintain the tool, to ensure that the Equifax Network is adequately monitored.
- **Logging and Monitoring:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing: (1) risk-based monitoring and logging of security events, operational activities, and transactions on the Equifax Network, (2) the reporting of anomalous activity through the use of appropriate platforms, and (3) requiring tools used to perform these tasks be appropriately monitored and tested to assess

proper configuration and maintenance. The Governance Process shall include the classification of security events based on severity and appropriate remediation timelines based on classification.

- **Vulnerability Scanning:** Equifax shall implement and maintain a risk-based vulnerability scanning program reasonably designed to identify and assess vulnerabilities within the Equifax Network.
- **Penetration Testing:** Equifax shall implement and maintain a risk-based penetration-testing program reasonably designed to identify and assess security vulnerabilities within the Equifax Network.
- **Vulnerability Planning:** Equifax shall rate and rank the criticality of all vulnerabilities within the Equifax Network. For each vulnerability that is ranked most critical, Equifax shall commence remediation planning within 24 hours after the vulnerability has been rated as critical and shall apply the remediation within one week after the vulnerability has received a critical rating. If the remediation cannot be applied within one week after the vulnerability has received a critical rating, Equifax shall identify or implement compensating controls designed to protect Personal Information as soon as practicable, but no later than one week after the vulnerability received a critical rating.
- **Patch Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process to maintain, keep updated, and support the software on the Equifax Network. Equifax shall maintain reasonable controls to address the potential impact that security updates and patches may have on the Equifax Network and shall maintain a tool that includes an automated Common Vulnerabilities and Exposures (CVE) feed with regular updates regarding known CVEs.
- **Threat Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing a threat management program designed to appropriately monitor the Equifax

Network for threats and assess whether monitoring tools are appropriately configured, tested, and updated.

- **Access Control and Account Management:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process established to appropriately manage Equifax Network accounts. This Governance Process shall include, at a minimum, (1) implementing appropriate password, multi-factor, or equivalent authentication protocols; (2) implementing and maintaining appropriate policies for the secure storage of Equifax Network account passwords, including policies based on industry best practices; and (3) limiting access to Personal Information by persons accessing the Equifax Network on a least-privileged basis.
- **File Integrity Monitoring:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process established to provide prompt notification of unauthorized modifications to the Equifax Network.
- **Legacy Systems:** Equifax shall develop and implement a risk-based plan to remediate current legacy systems on a schedule that provides for remediation within five years following final approval of this Agreement and which includes applying compensating controls until the systems are remediated. Equifax shall also maintain a Governance Process for active lifecycle management for replacing and deprecating legacy systems when they reach end of life.
- **Encryption:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process requiring Equifax either to encrypt Personal Information or otherwise implement adequate compensating controls.
- **Data Retention:** Equifax shall maintain, regularly review and revise as necessary, and comply with a Governance Process establishing a retention schedule for Personal Information on the Equifax Network and a process for deletion or destruction of Personal Information when such information is no

longer necessary for a business purpose, except where such information is otherwise required to be maintained by law.

- **TrustedID Premier:** Equifax, including by or through any partner, affiliate, agent, or third party, shall not use any information provided by consumers (or the fact that the consumer provided information) to enroll in TrustedID Premier to sell, upsell, or directly market or advertise its fee-based products or services.
- **Mandatory Training:** Equifax shall establish an information security training program that includes, at a minimum, at least annual information security training for all employees, with additional training to be provided as appropriate based on employees' job responsibilities.
- **Vendor Management:** Equifax shall oversee its third party vendors who have access to the Equifax Network by maintaining and periodically reviewing and revising, as needed, a Governance Process for assessing vendor compliance in accordance with Equifax's Information Security Program to assess whether the vendor's security safeguards are appropriate for that business, which Governance Process requires vendors by contract to implement and maintain such safeguards and to notify Equifax within 72 hours of discovering a security event, where feasible.
- **Incident Response Exercises:** Equifax shall conduct, at a minimum, biannual incident response plan exercises to test and assess its preparedness to respond to a security event.
- **Breach Notification:** Equifax shall comply with the state data breach notification laws, as applicable, and unless preempted by federal law.
- **Information Security Spending:** Equifax shall ensure that its Information Security Program receives the resources and support reasonably necessary for the Information Security Program to function as required by this Settlement. In addition, over a five-year period beginning January 1, 2019,

Equifax shall spend a minimum of \$1 billion on data security and related technology.

- **Third-Party Assessments:** Equifax shall engage a Third-Party Assessor meeting the criteria specified in this Agreement to conduct a SOC 2 Type 2 attestation, or to conduct an assessment using industry-recognized procedures and standards in satisfaction of Regulator requirements for this Agreement (the “Third-Party Assessments”).

Settlement Agreement, Exhibits 2 and 3.

45. In addition to the business practice changes regarding data security, Equifax has also agreed that it will not seek to enforce any arbitration provision or class action waiver in any Equifax product or service that has been offered in response to the breach or the settlement. Settlement Agreement ¶ 4.1.3. Further, Equifax will not receive any monetary or other financial consideration for the monitoring or restoration services made available under the Settlement, and is providing data necessary to provide those services free of charge. *Id.* ¶ 7.3.

The Notice Plan and Claims Process

46. A key feature of the settlement is a first-of-its-kind notice program that applies modern techniques used in commercial and political advertising to inform the class and stimulate participation. Settlement Agreement, Exhibit 6. The program, which was developed by Class Counsel and Signal Interactive Media with input from the Federal Trade Commission and Consumer Financial Protection

Bureau, consists of: (1) four emails to those class members whose email addresses can be found with reasonable effort, which is expected to be at least 75 percent of the class; (2) an aggressive digital and social media campaign designed to reach 90 percent of the class an average of eight times before the Notice Date and another six times by the end of the initial claims period; (3) radio advertising and a full-page, color advertisement in *USA Today* to reach those who have a limited digital presence; and (4) digital advertising during the extended claims period and while identity restoration services are available. *Id.*

47. The proposed emails and other notices, which are attached as exhibits to the Notice Plan, will be tested and targeted based on the demographics and other relevant characteristics of the class. The initial testing will involve focus groups, a national survey of 1,600 likely class members, and sending approved notices to small subsets of the class to measure their effectiveness. Then, once the full-scale campaign is launched, Signal will monitor its effectiveness through empirical data and continuously adjust the specific ads that are used and where those are placed to maximize their impact and drive claims. If the empirical data shows that additional measures are needed to accomplish its goals, the notice program may be supplemented with the Court's approval.

48. The claims process similarly draws upon the most up-to-date techniques to facilitate participation, including a link to a settlement website in all emails and digital advertising; the ability to file and check claims electronically optimized for use on any device whether mobile or via personal computer; and a call-center via a toll-free number to assist class members in filing claims. JND, the proposed Settlement Administrator, is a widely-regarded expert with the experience and capability to handle a case of this magnitude.

Attorneys' Fees and Expenses

49. Class Counsel may request a fee of up to \$77.5 million, which represents 25 percent of the original settlement fund created by the March 30 Term Sheet, and reimbursement of up to \$3 million in litigation expenses. Settlement Agreement ¶ 11.1. Equifax has agreed not to oppose this amount. *Id.* This provision was a separately negotiated provision of the Term Sheet and Settlement Agreement, which was not discussed until after the parties had agreed on relief to the class. Class Counsel believes this fee is justified as a percentage of the fund generated through its skill and efforts, and when considered in light of the substantial monetary and non-monetary benefits conferred on the Class.

50. Class Counsel will also seek service awards for \$2,500 for each Settlement Class Representative. Each of these individuals provided detailed

information of the circumstances regarding the impact of the breach that was vital to Class Counsel's investigation and litigation of the class's claims. Furthermore, each of them has remained active in the case, communicating with the attorneys working on the case during subsequent phases of the case. Equifax does not oppose these requests. *Id.* at ¶ 10.1. Both the application for fees and expenses, and the application for service awards will be filed at least 21 days before the Objection Deadline.

Releases

51. The class will release Equifax from claims that were or could have been asserted in this case and in turn Equifax will release the class from certain claims. *Id.* at ¶¶ 20-22. Class Counsel believes the releases are appropriately tethered to the claims that were presented in the litigation and therefore appropriate consideration in exchange for the substantial class relief provided by the settlement.

The Settlement is Fair, Reasonable, and Adequate

52. The resulting settlement, by any measure, is the largest settlement ever achieved in a data breach case. As reflected in the attached chart summarizing the terms of other significant consumer data breach settlements, the relief conferred on the class here including a non-reversionary fund of \$380.5 million

(plus an additional \$125 million if needed to pay Out-of-Pocket Losses and the added amount Equifax will have to pay for credit monitoring if more than 7 million class members enroll) is materially higher than that achieved in any other data breach case. Likewise, the specific benefits available to class members compare favorably to those available under any other settlement, and the business practice changes to which Equifax has agreed (including its commitment to spend at least \$1 billion on cybersecurity over the next five years) are far more extensive than have previously been achieved. *See* Exhibit 1.

53. Class Counsel also believes that a settlement at this point in the litigation is warranted because class members benefit immediately from protections like credit monitoring and identity restoration services that can help prevent and detect identity theft and fraud before misuse occurs, and assist class members in addressing any issues that arise, including the protection of a \$1 million insurance policy in case of identity theft or fraud.

54. Similarly, based on our experience in other data breach cases, the funds available in the Consumer Restitution Fund are tailored to address the losses stemming from the alleged breach. When a victim incurs out-of-pocket expenses relating to a data breach, it is typically associated with seeking advice about how to address the breach (e.g., paying for professional services), paying incidental costs

associated with identity theft or fraud (e.g., overdraft fees or costs for sending documents by certified mail), or taking mitigation measures like paying for credit monitoring or credit freezes. As such, the out-of-pocket expenses associated with a data breach are generally relatively modest, and rarely exceed several hundred dollars. When victims spend more than this amount, it is typically associated with paying for professional services such as accountant or attorneys' fees. As such, we believe the Settlement provides a mechanism to recover the out-of-pocket losses that would have been proved at trial.

55. The settlement must also be viewed against the significant risks to the Plaintiffs had they continued to litigate the case. There was a risk that Plaintiffs' claims would not have survived on a class-wide basis after a motion for class certification, or after one or more motions for summary judgment following the completion of fact and expert discovery. Data breach litigation is relatively new. While the law has gradually adapted, the path to a class-wide monetary judgment remains untrodden, and it will take some time before litigants and courts navigate all the unique issues posed by data breach lawsuits and some level of certainty sets, particularly in the area of damages.

56. Here, in addition to the traditional risks facing class plaintiffs in data breach cases, the settlement is highly beneficial when compared to two unique

risks presented under Georgia law, which the Court ruled applies to all the common law claims asserted by Plaintiffs. First, the Georgia Supreme Court recently called into question whether a defendant has a legal duty to safeguard the confidential personal information stolen in a data breach. *See Georgia Department of Labor v. McConnell* (Nos. S181786 and S181787), decided May 20, 2019. If this case was not settled (and had Equifax not executed a binding Term Sheet in March 2019), Equifax would have surely argued that the *McConnell* decision would bar Plaintiffs' common law claims under Georgia law.

57. Second, Equifax also argued in moving to dismiss that there are questions under Georgia law whether most class members suffered a legally-cognizable injury. In *Collins v. Athens Orthopedic Clinic*, 347 Ga. App. 13, 815 S.E.2d 13 (2018), the Georgia Court of Appeals specifically held that the costs of precautionary measures to protect against the risk of future harm from a criminal data breach are not recoverable under Georgia law. The Georgia Supreme Court has accepted cert in the case, but has yet to decide the case.

58. Class Counsel took all steps necessary to ensure that we had all the necessary information to advocate for a fair settlement that serves the best interests of the Settlement Class. Based on the public information available regarding the breach and Class Counsel's extensive review of the factual record produced by

Equifax, Class Counsel believes the Settlement is in the best interests of the Settlement Class.

59. Finally, there is no indication that there are any conflicts between the Settlement Class Representatives and the Settlement Class. Rather, Settlement Class Representatives' claims are substantially similar to the claims of the Settlement Class. Each of them was impacted by the Data Breach due to the unauthorized access to their personal information. Moreover, in crafting the Settlement, Class Counsel took care to ensure that the relief was allocated commensurate to the value of each class member's respective claims – those that suffered a greater Out-of-Pocket loss will be able to make a proportionately larger claim than someone that did not.

60. In light of the totality of the circumstances, including the historic relief provided to the class as described above, the Court should conclude that the settlement is fair, reasonable, and adequate and likely to achieve final approval, and therefore notice should issue to the class.

Continuing Appointment of Class Counsel

61. As discussed above, the Court previously appointed, Kenneth Canfield, Amy E. Keller, Norman E. Siegel and Roy Barnes as Class Counsel based on extensive applications provided to the Court. [Doc. 232] Class Counsel

respectfully submit that they have diligently served the class and the Court in litigating this case and presenting this Settlement for initial approval requesting issuance of notice and therefore request a continuing appointment pursuant to Fed. R. Civ. P. Rule 23(g) for purposes of implementing this Settlement.

We declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed this 21st day of July, 2019.

/s/ Kenneth S. Canfield
Kenneth S. Canfield

/s/ Amy E. Keller
Amy E. Keller

/s/ Norman E. Siegel
Norman E. Siegel

Chart of Data Breach Settlement Involving Class of 10+ Million

Case	Number of Class Members and PII Compromised	Monetary Settlement Benefits	Non-Monetary Security-Related Relief	Credit / Financial Acct. Monitoring
<p><i>In re: Yahoo! Inc. Customer Data Security Breach Litig.</i>, No. 16-md-02752-LHK (N.D. Cal.)</p> <p>Preliminary approval granted: July 20, 2019</p>	Up to 194 million individuals w/ compromised email addresses, passwords, security questions and answers, and telephone numbers and dates of birth if provided	<ul style="list-style-type: none"> • \$117.5 million cash fund which includes: • Reimbursement of class members' out-of-pocket costs up to \$25,000 and time spent remediating issues up to 15 hours with documentation and 5 hours without documentation at \$25 per hour • Alternative payments to class members w/ credit monitoring for \$100 (can be increased to \$358.80 per individual) • 2 years of credit monitoring (to be extended if remaining funds) • Compensate paid users of Yahoo! for up to 25% of the amounts they paid for email services • Attorneys fees' up to \$30 million and costs and expenses up to \$2.5 million • Notice and administration costs up to \$6 million 	<ul style="list-style-type: none"> • Increased security budget and security employee headcount • Implementation of security program compliant with NIST Cybersecurity Framework • Four years of third-party risk assessments • Implementation of vulnerability management schedules requiring critical issues to be resolved on set schedule • Implementation of enhanced intrusion and anomaly detection tools • Employee security training • Appointment of external Chief Information Security Officer board of advisors 	Yes, 2 years of credit monitoring through AllClear ID that may be extended multiple years depending on remaining funds
<p><i>In re: Experian Data Breach Litig.</i>, No. 8:15-cv-01592 (C.D. Cal.)</p>	14.93 million individuals w/ compromised names, addresses, SSNs,	<ul style="list-style-type: none"> • \$22 million cash fund which includes: • Reimbursement of class members' 	<ul style="list-style-type: none"> • Data security enhancements to Experian's network • Remediation of identified 	Yes, 2 years of credit monitoring through Identity Guard that may be extended if

Final approval granted: May 30, 2019	dates of birth, identification numbers, and other PII	<p>out-of-pocket costs up to \$10,000 and time spent remediating issues up to 7 hours with documentation and 2 hours without documentation at \$20 per hour</p> <ul style="list-style-type: none"> • 2 years of credit monitoring at cost of up to \$2.5 million depending on number of claimants • Attorneys fees' up to \$10.5 million and costs and expenses up to approx. \$153,000 	<p>vulnerabilities</p> <ul style="list-style-type: none"> • Heightened encryption throughout network and user database • Implementation of Security First Program consisting of 82 security-related projects • Hiring an additional 60 full-time security employees 	certain conditions are met
<p><i>In re: Anthem, Inc. Data Breach Litig.</i>, No. 15-md-02617-LHK (N.D. Cal.)</p> <p>Final approval granted: Aug. 15, 2018</p>	79.15 million individuals w/ compromised names, dates of birth, SSNs, healthcare ID numbers, addresses, and other PII	<ul style="list-style-type: none"> • \$115 million cash fund which includes: • Reimbursement of class members' out-of-pocket costs up to \$10,000 (up to \$15 million of fund allocated for this purpose) • Alternative payments to class members w/ credit monitoring for \$50 (up to \$13 million of fund allocated for this purpose) • Access to fraud resolution services through Experian for all class members • 2 years of credit monitoring at a cost of \$17 million (to be extended 	<ul style="list-style-type: none"> • Increased annual spending on data security for three years • Implement cybersecurity controls and reforms recommended by Plaintiffs' cybersecurity experts • Change data retention policies • Follow specific remediation recommendations • Perform annual IT security risk assessments and settlement compliance review 	Yes, 2 years of credit monitoring through Experian that may be extended multiple years depending on remaining funds

		if remaining funds) <ul style="list-style-type: none"> Attorneys fees' up to \$37.95 million and costs and expenses up to \$2.14 million¹ Notice and administration costs of \$23 million 		
<i>In re: The Home Depot, Inc. Consumer Data Security Data Breach Litig.</i> , No. 1:14-md-02583 (N.D. Ga.) Final approval granted: Aug. 23, 2016	40 million individuals with compromised payment card information Up to 53 million with stolen email addresses	<ul style="list-style-type: none"> \$13 million cash fund \$6.5 million for credit monitoring services separate from cash fund Up to \$8.475 million in attorneys' fees and \$300,000 in costs separate from cash fund² Notice and administration costs of \$750,000 separate from cash fund Total Value: 29,025,000 ³	<ul style="list-style-type: none"> Appointment of Chief Information Security Officer Required product and data risk assessments Heightened vendor selection Dynamic security program implementation Employee education Enhanced security measures for payment cards 	Yes, 18 months of identity protection services from Identity Guard
<i>In re: Target Corp. Customer Data Sec. Breach Litig.</i> , No. 14-md- 2522 (D. Minn.) Final approval granted: Nov. 15,	Up to 110 million individuals with compromised payment card information	<ul style="list-style-type: none"> \$10 million cash fund Notice and administration costs of \$6.57 million separate from cash fund Up to \$6.75 million in attorneys' fees separate from cash fund Total Value: \$23,320,816 ⁴	<ul style="list-style-type: none"> Appointment of Chief Information Security Officer Maintain written information security program Maintain process to 	No

¹ The full amount of fees and costs were not ultimately awarded.

² *Home Depot*, ECF No. 181-2 at ¶¶ 28, 38, 61.

³ The full amount of fees and costs were not ultimately awarded, resulting in an actual total value of \$28,468,800.97.

2015 (affirmed on appeal June 14, 2018)			monitor for and respond to information security events <ul style="list-style-type: none"> Employee security training 	
<i>In re Sony Gaming Networks and Consumer Data Security Breach Litig.</i> , No. 3:11-md-02258 (S.D. Cal.) Final approval granted: May 4, 2015	60 million individuals w/ compromised names, mailing addresses, email addresses, dates of birth, credit card information, login credentials, answers to security questions, purchase history	<ul style="list-style-type: none"> No fund; claims-made settlement capped at \$1 million with additional non-cash benefits Reimbursement up to \$2,500 for class members with unreimbursed charges from identity theft (capped at \$1 million) \$14 million in non-cash benefits including free games, subscriptions, and credits for various subclasses Notice and administration costs of \$1.25 million to be paid separately Attorneys fees' up to \$2.67 million and costs and expenses of \$77,724 to be paid separately 	No	No
<i>In re: Heartland Payment Systems, Inc. Customer Data Security Breach Litig.</i> , 4:09-MD-2046 (S.D. Tex.) Final approval granted: March 20,	130 million individuals w/ compromised payment card information	<ul style="list-style-type: none"> Settlement fund of \$1 million and up to \$2.4 million depending on number of claims Reimbursement of class members' out-of-pocket costs up to \$175 or \$10,000 in cases of identity theft and time spent remediating issues up to 5 hours with documentation at \$10 per hour 	<ul style="list-style-type: none"> Class Counsel employed independent expert to review the actions taken by Heartland to enhance the security of its payment processing systems and determined Heartland took prudent and good faith measures to minimize likelihood of a future 	No

⁴ *Target*, ECF No. 482 at 35; *see also* ECF No. 645 at 8 (Final Approval Order) (noting that fee award of \$6.75 million was 29% of total monetary fund, equating to value of 23,275,862).

2012		<ul style="list-style-type: none"> Attorneys fees' up to \$725,000 and costs and expenses up to \$35,000 to be paid separately 	intrusion	
<p><i>In re: Countrywide Financial Corp. Customer Data Security Breach Litig.</i>, No. 3:08-MD-01998 (W.D. Ky.)</p> <p>Final approval granted: Aug. 23, 2010</p>	17 million individuals w/ compromised names, SSNs, addresses, telephone numbers, credit and bank account information, and other financial information	<ul style="list-style-type: none"> No fund; claims-made settlement capped at \$6.5 million Reimbursement of losses attributable to identity theft up to \$50,000 per incident (capped at \$5 million) Reimbursement of out-of-pocket expenses incurred as result of identity theft (capped at \$1.5 million) Notice and administration costs of approx. \$6 million to be paid separately Attorneys fees' up to \$3.5 million and costs and expenses up to \$125,000 to be paid separately Service awards totaling \$26,500 to be paid separately 	<ul style="list-style-type: none"> Enhanced security measures adopted by Countrywide and subject to confirmatory discovery 	Yes, 2 years of credit monitoring services from Experian offered to 1.85 million class members who did not receive prior offer from Countrywide
<p><i>In re Department of Veterans Affairs (VA) Data Theft Litig.</i>, No. 06-0506 (JR) (D.D.C.)</p> <p>Final Approval granted: Sept. 11, 2009</p>	26.5 million individuals with compromised names, dates of birth, and SSNs	<ul style="list-style-type: none"> Settlement fund of \$20 million Reimbursement of class members' out-of-pocket costs up to \$1,500 with each claimant to receive a minimum of \$75 Balance paid to targeted military <i>cy pres</i> recipients Notice and administration costs to be paid from fund 	No	No

		<ul style="list-style-type: none"> Attorneys fees' of \$3.6 million and costs and expenses of \$157,076 awarded from fund 		
<p><i>In re TJX Companies Retail Security Breach Litig.</i>, No. 07-10162 (D. Mass.)</p> <p>Final approval granted: Sept. 2, 2008</p>	45.7 million individuals with compromised payment card information	<ul style="list-style-type: none"> No fund; claims-made settlement capped at \$10 million \$15 check or \$30 store voucher for class members who certify they made a purchase at TJX and spent more than \$5 or 30 minutes as a result of the data breach (subject to \$10 million cap with checks and vouchers credited as \$30 against cap) Additional \$15 check or \$30 voucher for documented claims (\$7 million cap on checks, no cap on vouchers) Reimbursement of driver's license replacement costs and unreimbursed losses greater than \$60 resulting from identity theft available to approx. 455,000 class members whose ID was compromised Notice and administration costs of approx. \$4.5 million to be paid separately Attorneys fees' up to \$6.5 million and costs and expenses up to \$155,000 to be paid separately 	<ul style="list-style-type: none"> Retain an independent expert to recommend data security practices to be adopted by TJX and accepted by Plaintiffs' expert Enhanced computer systems 	Yes, 3 years of credit monitoring services from Equifax for the approx. 455,000 class members whose driver's license or military, tax or state identification number may have been compromised